SOC for Cybersecurity

In April 2017, the American Institute of Certified Public Accountants (AICPA) released a new framework for cybersecurity risk management that can help businesses meet the growing challenges that they face from cybersecurity threats. The purpose of this whitepaper is to provide answers to some of the frequently asked questions that Kfi receives about the new framework and the related examination.

Question #1:

What exactly is "SOC for Cybersecurity"?

Answer #1:

System and Organization Controls (SOC) for Cybersecurity is a market-driven, flexible, and voluntary reporting framework that helps organizations communicate about their cybersecurity risk management programs and the effectiveness of program controls and for CPAs to examine and report on such information. It uses a common, underlying language, or framework, for cybersecurity risk management reporting, to enable all organizations, in all industries, to communicate relevant information about their cybersecurity risk management programs..

Question #2:

What is a SOC for Cybersecurity Examination?

Answer #2:

SOC for Cybersecurity is an examination engagement performed by CPAs on an entity's cybersecurity risk management program.The AICPA Guide, *Reporting on an Entity's Cybersecurity Risk Manage-ment Program and Controls*, provides guidance for practitioners engaged to examine and report on an entity's cybersecurity risk management program. In a cybersecurity risk management examination, the practitioner / CPA opines on: (a) management's description of the entity's cybersecurity risk management program and (b) the effectiveness of controls within that program to achieve the entity's cybersecurity objectives. A cybersecurity risk management examination results in the issuance of a general use cybersecurity report designed to meet the needs of a variety of potential users.

Question #3:

Wait a minute! How does the new framework differ from Service Organization Controls reports? These are also called "SOC." Couldn't the AICPA come up with a different acronym?

Answer #3:

The new framework and related examination are focused exclusively on cybersecurity risk management and controls across the entire organization. A Service Organization Controls report, on the other hand, is generally focused on a broader set of controls related to specific products or services. However, there are similarities in the types of information and controls that appear in the new SOC for Cybersecurity and the traditional SOC 2 report, particularly around the security, availability and confidentiality principles. Common controls in the 2 reports will include firewalls, intrusion detection and intrusion prevention systems, penetration testing, vulnerability scanning, logging / monitoring, passwords and security settings, controls related to granting and removing system access, etc. In essence, most of the key technical controls from the traditional SOC report will also appear in a SOC for Cybersecurity report.

Question #4:

What types of organizations is SOC for Cybersecurity intended for?

Answer #4:

The framework and related examination can be used by any type of business. While the traditional Service Organization Controls (SOC) reports are only intended for businesses defined as "service organizations," the new framework is applicable to all entities.

Question #5:

Who are the potential users of the cybersecurity examination report and what are the benefits of the report?

Answer #5:

The potential users of the report and the benefits they will receive include the following:

- **Senior management:** A cybersecurity risk management examination report provides senior management with information about the effectiveness of an organization's cybersecurity risk management program, including the controls designed, implemented and operated to mitigate threats against the entity's sensitive information and systems.

- **Boards of directors:** A cybersecurity risk management examination report provides board members with information about the cybersecurity risks the entity faces and the program that management has implemented to help them fulfill its oversight responsibilities. It also helps them evaluate management's effectiveness in managing cybersecurity risks.

- **Analysts and investors:** A cybersecurity risk management examination report provides analysts and investors with information about an entity's cybersecurity risk management program. This information is intended to help them understand the cybersecurity risks that could threaten

the achievement of the entity's operational, reporting, and compliance (legal and regulatory) objectives and, consequently, have an adverse impact on the entity's value and stock price.

- **Business partners:** A cybersecurity risk management examination report provides business partners with information about the entity's cybersecurity risk management program as part of their overall risk assessment. This information may help determine matters such as whether there is a need for multiple suppliers for a good or service and the extent to which they choose to extend credit to the entity. Some business partners may need a detailed understanding of controls implemented by the entity and the operating effectiveness of those controls to enable them to design and operate their own control activities. For example, business partners whose information technology (IT) systems are interconnected with systems at the entity may need to understand the specific logical access protection over the interconnected systems implemented by the entity.

Question #6:

What are the components of a cybersecurity risk management examination report?

Answer #6:

The cybersecurity risk management examination report includes the following three key components:

- **Management's description of the entity's cybersecurity risk management program.** The first component is a management-prepared narrative description of the entity's cybersecurity risk management program (description). This description is designed to provide information about how the entity identifies its information assets, the ways in which the entity manages the cybersecurity risks that threaten it, and the key security policies and processes implemented and operated to protect the entity's information assets against those risks. The description provides the context needed for users to understand the conclusions, expressed by management in its assertion and by the practitioner in his or her report. Management uses the description criteria to prepare and evaluate an entity's cybersecurity risk management program.

- **Management's assertion.** The second component is an assertion provided by management, which may be as of a point in time or for a specified period of time. Specifically, the assertion addresses whether (a) the description is presented

in accordance with the description criteria and (b) the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria. The AICPA has developed control criteria for use when evaluating whether the controls within the program were effective to achieve the entity's cybersecurity objectives.

- **Practitioner's report.** The third component is a practitioner's report, which contains an opinion, which addresses both subject matters in the examination. Specifically, the opinion addresses whether (a) the description is presented in accordance with the description criteria and (b) the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Question #7: Is the report as of a point in time or over a period?

Answer #7: Similar to a Type 1 and Type 2 SOC report, the cybersecurity report can be as of a point in time or over a period.

Question #8: Does Kfi perform SOC for Cybersecurity examinations?

Answer #8: Yes - Kfi performs SOC for Cybersecurity examinations. The firm delivers Service Organization Controls reports to hundreds of entities and will leverage this background, as well as our IT audit and cybersecurity expertise in delivering these services.